

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently Amended) An automated method of preventing an
2 endnode in a communication fabric from receiving an unauthorized
3 communication, comprising:
4 establishing a first category of management communications to include:
5 a request from a manager node to an endnode; and
6 a reply from the manager node to a request from an endnode;
7 establishing a second category of management communications to
8 include:
9 a reply from an endnode to a request from the manager node; and
10 a request from an endnode to the manager node; and
11 at a switching device coupled to a first endnode:
12 receiving from the communication fabric a management
13 communication packet addressed to the first endnode;
14 determining whether the first endnode is a trusted endnode;
15 determining whether the management communication is a first
16 category management communication based on ~~a management class of the~~
17 ~~node whether~~ the management communication is originated from a
18 ~~manager node~~ and whether the management communication is a request or
19 a reply; and
20 responsive to if the first endnode not being is not a trusted endnode
21 and the management communication not being a first category

22 ~~management communication,~~ discarding the management
23 communication ~~if the management communication is not a first category~~
24 ~~management communication.~~

1 2. (Original) The method of claim 1, further comprising:
2 classifying each endnode in the communication fabric as either trusted or
3 untrusted.

1 3. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 associating with each port of the switching device an indicator configured
4 to indicate whether a node coupled to the port is trusted.

1 4. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 classifying the first endnode as a trusted endnode if the first endnode is a
4 manager node.

1 5. (Original) The method of claim 2, wherein said classifying
2 comprises:
3 classifying the first endnode as an untrusted endnode if the first endnode is
4 not configured to act as a manager node.

1 6. (Original) The method of claim 1, wherein said determining
2 comprises:
3 reading an indicator associated with a port of the switch to which the first
4 endnode is coupled;
5 wherein said indicator is configured to indicate whether the first endnode

6 is trusted.

1 7. (Currently Amended) The method of claim 1, further comprising,
2 at the switching device:

3 ~~If responsive to the first endnode being a is-trusted endnode~~, forwarding
4 the management communication to the first endnode regardless of the category of
5 the management communication.

1 8. (Currently Amended) The method of claim 1, further comprising,
2 at the switching device:

3 receiving a second management communication from the first endnode;
4 and

5 responsive to the management communication not being a second
6 category management communication, discarding the second management
7 communication ~~if the management communication is not a second category~~
8 ~~management communication~~.

1 9. (Original) The method of claim 1, wherein the communication
2 fabric comprises a subnet of an InfiniBand communication fabric.

1 10. (Original) The method of claim 9, wherein a management
2 communication comprises a communication transmitted on virtual lane 15 of the
3 InfiniBand communication fabric.

1 11. (Currently Amended) A computer readable medium storing
2 instructions that, when executed by a computer, cause the computer to perform a
3 method of preventing an endnode in a communication fabric from receiving an
4 unauthorized communication, comprising:

5 establishing a first category of management communications to include:
6 a request from a manager node to an endnode; and
7 a reply from the manager node to a request from an endnode;
8 establishing a second category of management communications to
9 include:
10 a reply from an endnode to a request from the manager node; and
11 a request from an endnode to the manager node; and
12 at a switching device coupled to a first endnode:
13 receiving from the communication fabric a management communication
14 addressed to the first endnode;
15 determining whether the first endnode is a trusted endnode;
16 determining whether the management communication is a first
17 category management communication based on ~~a management class of the~~
18 ~~node~~whether the management communication is originated from a
19 manager node and whether the management communication is a request or
20 a reply; and
21 ~~if responsive to the first endnode not being is not~~ a trusted endnode
22 ~~and the management communication not being a first category~~
23 ~~management communication~~, discarding the management communication
24 ~~if the management communication is not a first category management~~
25 ~~communication.~~

1 12. (Currently Amended) An automated method of preventing an
2 endnode in a communication fabric from sending an unauthorized
3 communication, comprising:
4 establishing a first category of management communications to include:
5 a request from a manager node to an endnode; and
6 a reply from the manager node to a request from an endnode;

7 establishing a second category of management communications to
8 include:
9 a reply from an endnode to a request from the manager node; and
10 a request from an endnode to the manager node; and
11 at a switching device coupled to a first endnode:
12 receiving from a first endnode a management communication addressed to
13 a second endnode in the communication fabric;
14 determining whether the first endnode is a trusted endnode;
15 determining whether the management communication is a second
16 category management communication based on ~~a management class of the~~
17 ~~node whether the management communication is destined for~~ originated
18 ~~from a manager node~~ and whether the management communication is a
19 request or a reply; and
20 ~~if responsive to the first endnode is not being a trusted endnode and~~
21 ~~the management communication not being a second category management~~
22 ~~communication,~~ discarding the management communication if the
23 ~~management communication is not a second category management~~
24 ~~communication.~~

1 13. (Original) The method of claim 12, further comprising:
2 classifying each endnode in the communication fabric as either trusted or
3 untrusted.

1 14. (Original) The method of claim 12, wherein said classifying
2 comprises:
3 associating with each port of the switching device an indicator configured
4 to indicate whether a node coupled to the port is trusted.

1 15. (Currently Amended) The method of claim 12, wherein said
2 classifying comprises:
3 responsive to the first endnode being a manager node, classifying the first
4 endnode as a trusted endnode ~~if the first endnode is a manager node~~.

1 16. (Currently Amended) The method of claim 12, wherein said
2 classifying comprises:
3 responsive to the first endnode not being configured to act as a manager
4 node, classifying the first endnode as an untrusted endnode ~~if the first endnode is~~
5 ~~not configured to act as a manager node~~.

1 17. (Original) The method of claim 12, wherein said determining
2 comprises:
3 reading an indicator associated with a port of the switch to which the first
4 endnode is coupled;
5 wherein said indicator is configured to indicate whether the first endnode
6 is trusted.

1 18. (Currently Amended) The method of claim 12, further comprising,
2 at the switching device:
3 responsive to if the first endnode being a is-trusted endnode, forwarding
4 the management communication toward the second endnode regardless of the
5 category of the management communication.

1 19. (Currently Amended) The method of claim 12, further comprising,
2 at the switching device:
3 receiving a second management communication addressed to the first
4 endnode; and

5 responsive to the management communication not being a first category
6 management communication, discarding the second management communication
7 if the management communication is not a first category management
8 communication.

1 20. (Original) The method of claim 12, wherein the communication
2 fabric comprises a subnet of an InfiniBand communication fabric.

1 21. (Original) The method of claim 20, wherein a management
2 communication comprises a communication transmitted on virtual lane 15 of the
3 InfiniBand communication fabric.

1 22. (Currently Amended) A computer readable medium storing
2 instructions that, when executed by a computer, cause the computer to perform a
3 method of preventing an endnode in a communication fabric from sending an
4 unauthorized communication, comprising:
5 establishing a first category of management communications to include:
6 a request from a manager node to an endnode; and
7 a reply from the manager node to a request from an endnode;
8 establishing a second category of management communications to
9 include:
10 a reply from an endnode to a request from the manager node; and
11 a request from an endnode to the manager node; and
12 at a switching device coupled to a first endnode:
13 receiving from a first endnode a management communication addressed to
14 a second endnode in the communication fabric;
15 determining whether the first endnode is a trusted endnode;
16 determining whether the management communication is a second

17 category management communication based on ~~a management class of the~~
18 ~~node~~whether the management communication is destined for~~or~~originated
19 ~~from a manager node~~ and whether the management communication is a
20 request or a reply; and
21 responsive to if~~the first endnode is not being~~ a trusted endnode,
22 discarding the management communication if the management
23 communication is not a second category management communication.

1 23. (Currently Amended) An apparatus for preventing a node in a
2 communication fabric from engaging in unauthorized communication, the
3 apparatus comprising:
4 a switching device configured to route management communications
5 through the communication fabric, wherein:
6 a type one management communications comprise requests from a
7 manager node to endnodes and replies from the manager node to requests
8 from endnodes; and
9 a type two management communications comprise replies from
10 endnodes to requests from the manager node and requests from
11 endnodes to the manager node;
12 wherein a management communication is categorized to be a type
13 one or a type two management communication based on ~~a management~~
14 ~~class of the node~~whether the management communication is ~~originated~~
15 ~~from or destined for a manager node~~ and whether the management
16 communication is a request or a reply ;
17 for each port of the switching device, an indicator configured to indicate
18 whether an endnode coupled to the port is trusted;
19 wherein a first management communication addressed to a first endnode
20 coupled to a first port of the switching device is discarded responsive to the first

21 endnode not being a trusted endnode and the first management communication
22 not being a type one management communication if the first endnode is not
23 trusted and the first management communication is not a type one management
24 communication; and
25 wherein a second management communication received from the first
26 endnode is discarded responsive to if the first endnode is not being a trusted
27 endnode and the second management communication is not being a type two
28 management communication.

1 24. (Original) The apparatus of claim 23, further comprising:
2 a secure channel configured to allow a management node to configure said
3 indicators.

1 25. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to another switching element, said indicator is set to
3 indicate the other switching element is trusted.

1 26. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to a management node, said indicator is set to
3 indicate the management node is trusted.

1 27. (Original) The apparatus of claim 23, wherein:
2 for each port coupled to an endnode that is not configured to act as a
3 management node, said indicator is set to indicate the endnode is not trusted.

1 28. (Original) The apparatus of claim 23, wherein:
2 the communication fabric comprises an InfiniBand communication fabric;
3 and

4 a management communication comprises a communication transmitted
5 over virtual lane 15 of the InfiniBand communication fabric.

1 29. (Currently Amended) A computer readable medium residing in a
2 communication switch and containing a data structure configured for indicating
3 trust, the data structure comprising:
4 for each port of the communication switch, an indicator configured to
5 indicate whether a communication node coupled to the port is trusted;
6 wherein a port indicator is set to a first state responsive to ~~if~~ the coupled
7 communication node being a ~~is~~ trusted node and is set to a second state
8 responsive to ~~if~~ the coupled communication node ~~is not~~ being a ~~trusted node~~; and
9 wherein management communications addressed to the coupled
10 communication node are filtered based on ~~a management class of the~~
11 ~~node whether~~ the management communication is ~~is~~ originated from or destined to a
12 manager node and whether the management communication is a request or a reply
13 if the port indicator is set to said second state.